Mobility Reduces Uncertainty in MANETs

Feng Li and Jie Wu
Department of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL 33431

Abstract— **Evaluating and quantifying trust stimulates collaboration in mobile ad hoc networks (MANETs). Many existing reputation systems sharply divide the trust value into right or wrong, thus ignore another core dimension of trust: uncertainty. As uncertainty deeply impacts a node's anticipation of others' behavior and decisions during interaction, we include uncertainty in the reputation system. Specifically, we use an uncertainty metric to directly reflect a node's confidence in the sufficiency of its past experience, and study how the collection of trust information may affect uncertainty in nodes' opinions. Higher uncertainty leads to higher transaction cost and reduced acceptance of communication and cooperation. After defining a way to reveal and compute the uncertainty in trust opinions, we exploit mobility, one of the important characteristics of MANETs, to efficiently reduce uncertainty and to speed up trust convergence. A two-level Mobility Assisted Uncertainty Reduction Scheme (MAURS) that offers controllable trade-off between time and cost to achieve a trust a convergence objective is also provided. Extensive analytical and simulation results are presented to support our proposal.**

Keywords: Mobile ad hoc networks (MANETs), mobility, trust evaluation, uncertainty.

I. Introduction

Mobile ad hoc networks (MANETs) aim to provide wireless network services without relying on any infrastructure. The main challenge in MANETs comes from their self-organized and distributed nature. There is an inherent reliance on collaboration between the participants of a MANET in order to achieve the aimed functionalities. Collaboration is productive only if all participants operate in an honest manner. Therefore, establishing and quantifying trust, which is the driving force for collaboration, is important for securing MANETs.

Trust can be defined as the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context. It represents a MANET participant's anticipation of other nodes' behavior when assessing the risk involved in future interactions. Here the participant is usually called trustor, and other nodes are called the trustee. The trust relationship usually builds on the basis of the trustor's past direct interaction experiences and others' recommendations related to the trustee. The abstracted value from past experiences and recommendations is defined as the trustee's reputation.

Many reputation systems have been proposed in the literature, most of them sharply divide the recorded behavioral information into right or wrong. For example, in the EigenTrust model [1], behavioral information is obtained by counting the number of 'satisfactory' and 'unsatisfactory' interactions, and the difference between these two values is stored as reputation record. Besides lacking a precise semantic, this information has abstracted away any notion of time. In EigenTrust, value 0 may represent both 'no past interaction' and 'many unsatisfactory past interactions'. Consequently, one cannot verify exact properties of past behavior based on this information alone.

To tackle this problem, we introduce the concept of uncertainty, expand the subjective logic [2], and design a certainty oriented reputation system to rationally evaluate trust. Uncertainty refers to the degree to which an individual or organization cannot accurately predict the behavior of its mutual rival or the environment. Uncertainty originates from information asymmetry and opportunism. It reflects whether a trustor has collected enough information from past interactions with a trustee and its confidence in that information. After adding this core dimension of trust into our reputation system, we can clearly separate newcomers from misbehavers, and make certainty based decisions possible. A series of uncertainty deduction formulas is also provided to rationally combine the trustor's first-hand observation with the collected second-hand recommendations.

Uncertainty increases transaction cost and decreases acceptance of communication and cooperation. Our objective is to reduce the trustor's perceived uncertainty so that transaction cost is lowered and a long-term exchange relationship is sustained. A way to efficiently reduce uncertainty is to exploit one important property of MANETs: mobility. Node movement can increase the scope of direct interaction and recommendation propagation, hence speed up trust convergence. We study this effect under different mobility models and analyze several factors which will strongly influence the convergence speed and cost. We present a detailed design of a two-level Mobility Assisted Uncertainty Reduction Scheme (MAURS). It exploits configurable level partition and movement schemes to provide a range of trade-offs between convergence time, cost and uncertainty level. MAURS offers flexibility for users to achieve their application objectives.

The contributions of this paper are as follows:

1) We rigorously define the concept of uncertainty, and its role in trust evaluation.
2) We propose a certainty oriented reputation system. Each node uses the Beta function to evaluate its first-hand observation, synthesizes the second-hand recommendations with a weighted average method, and combines information into belief, disbelief and uncertainty.
3) We analyze the uncertainty reduction effects under var-

ious mobility scenarios. We present a controlled hierarchical movement model that can efficiently reduce uncertainty and speed up trust convergence.

The remainder of this paper is organized as follows. Section II discusses several related solutions. Section III introduces the detailed design of our certainty oriented reputation model. We analyze the effect of mobility on uncertainty reduction in Section IV. In Section V, we discuss some implementation issues and Section VI presents the simulation results. Finally, Section VII concludes this work and outlines future work.

II. Related Work

A. Trust Management Systems

Various frameworks [3] [4] [5] have been designed to model trust networks and have been used as trust management systems. We can divide them into three main categories. The trust management system in the first category has a central authority, which is usualy called the trusted third party (TTP). Entities cooperate on the basis of the trust values (e.g. the authorization certificates) assigned by the TTP. Introducing a TTP will violate the self-organized nature of MANETs which makes these systems inapplicable in MANETs.

In the second category, one global trust value is drawn and published for each node, based on other nodes' opinion towards it. EigenTrust [1] is one mechanism in this category. The algorithm allows computation of global trust values in the distributed environment. EigenTrust presents the request to separate misbehavers from newcomers. But it lacks the method to satisfy this request naturally. EigenTrust is just a representative and most existing trust evaluation systems have the same requirement but omit uncertainty at the same time.

The third category is the trust management systems that allow each node to have its own view of other nodes. These systems are more realistic as they are similar to the trust models in the social network. Each node builds its view based on the observation as well as the recommendations from others. Many recent reputation systems such as CONFIDANT [6], CORE [7] and OCEAN [8] belong to this category. In the improved CONFIDANT [9], Buchegger et al. provided a modified Bayesian approach for reputation representation, updates, and view integration. When updating the reputation according to recommendations, only information that is compatible with the current reputation rating is accepted. This approach is objective and robust. But this approach still leaves an opportunity for elaborate attackers to launch false accusation attacks since there is no constraint on update frequency. This approach also lacks the ability to separate newcomers from misbehavers.

Josang [2] [10] [11] developed an algebra for assessing trust relations, and it has been applied to set up certification chains. In this algebra, the focus is on modeling the uncertainty in the reputation. A triplet designating belief, disbelief, and uncertainty is assigned to each trust statement. Many operators are given for the manipulation of these opinions. This model's strength lies in its ability to reason about the opinions and its consensus, recommendation, and ordering operators. However, its major weakness is that every entity's opinion is based on its own subjective policy and the system cannot guarantee that users will assign consistent values. It also lacks an operator to synthesize different recommendations, or combine first-hand and second-hand opinions into one metric.

B. The Effect of Mobility on Security

Mobility is one of the important characteristics of MANETs [12], and trust evaluation is an important method to stimulate nodes in MANETs to cooperate. However, to the best of our knowledge, there is no literature that fully addresses mobility's influence on trust convergence.

In [13], Wu presents the question whether mobility should be treated as a foe (undesirable) or a friend (desirable). In security related research, this question also attracted a significant amount of research interests [14] [15] [16]. Some researchers argue that mobility is a hurdle to security, as it makes the authentication and identification process more difficult. Some new mechanisms such as [16] have been proposed to tackle the problems caused by node mobility in MANETs. Others argue that far from being a hurdle, mobility can be exploited to set up security associations among users. In [15], Capkun et al. provide a method that leverages the temporary vicinity of users and runs appropriate cryptographic protocols to allow users to exchange certificates based on this vicinity. They study the pace of establishment of security associations under various mobility scenarios. It is the first research effort which shows how mobility can help to secure and accelerate key exchange in MANETs.

III. Certainty Oriented Reputation System

A. Motivations and Assumptions

Uncertainty is an important factor in trust evaluation. How to fully address and model uncertainty, and make it a direct metric is a key problem in trust evaluation system design and implementation. Another problem is to efficiently reduce uncertainty once we know how to evaluate it. In social life, if people want to raise their confidence in the evaluation of someone, they just get closer to that person and create chances for direct contact, or take the recommendations from someone they trust who knows the subject better. In MANETs, mobility increases the chance that two separated nodes meet and directly contact. It also allows each node to have more evidence to verify future recommendation. Intuitively, we consider mobility to be a good choice to reduce uncertainty.

In this paper, the following assumptions were made: Each node has one unique ID and it cannot be spoofed; A node can only monitor the behavior of its one hop neighbor. When two nodes directly contact each other in one hop, they have a way to decide whether the result is satisfactory; Nodes' behavior are consistent. A node's general behavior can be deducted from its past actions; Nodes are independent from each other, with no collusion. Our reputation system can accommodate independent false praise and false accusation.

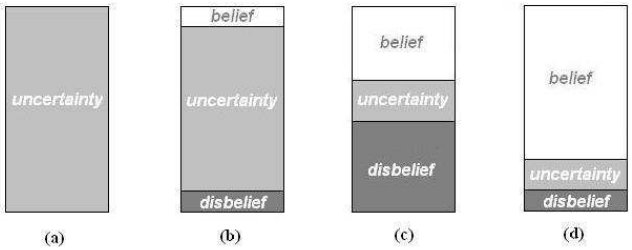


Fig. 1. Reputation representation.

B. Reputation Representation

The representation of reputation reflects the focus of a trust evaluation system. Reputation is the opinion of one entity towards another based on past experiences. In most of the existing systems, reputation is represented as two variables: belief and disbelief. However, dividing trust into only belief or disbelief is not always appropriate. One reputation value based on ten contact experiences and another based on one hundred contact experiences have totally different meanings. An information ordering between no knowledge and total certainty is needed to reflect the degree of confidence in trust information.

In this system, an one-dimensional representation of belief, disbelief and uncertainty is extended from the subjective logic [2]. Each node keeps a belief and disbelief value towards other nodes as a prediction of their future behavior. As these two value are only predictions, uncertainty always exists. We use a triplet to represent a node's opinion $(b, d, u) \in [0, 1]^3 : b+d+u = 1$. b, d, and u designate belief, disbelief, and uncertainty respectively.

C. First-hand Information Gathering

The reputation of a node computed from first-hand information is the reputation based on one's own experience. It is calculated directly from a node's observation. Each node will also propagate this information so that other nodes can use it as second-hand information. Each node estimate its neighbor's reliability based on its accumulated observations using Bayesian inference.

Bayesian inference is statistical inference in which evidence or observations are used to update or to newly infer the probability that a hypothesis may be true. Beta distributions, $Beta(\alpha, \beta)$, are used here in the Bayesian inference, since it only needs two parameters that are continuously updated as observations are made. To start with, each node in the network has the prior $Beta(1, 1)$ for all its neighbors. The prior $Beta(1, 1)$ implies that the distribution of the reliability metric p complies with the uniform distribution on $[0, 1]$, which indicates complete uncertainty as there are no observations. When a new observation is made, if it is a successful forwarding, then α is updated. Otherwise, β is updated. The prior is then updated as $Beta(\alpha, \beta)$ when needed. As we use a triplet to represent the node's opinion, the triplet (b, d, u) is derived from $Beta(\alpha, \beta)$. Fig. 2 shows that different $\alpha + \beta$ influence the density of the distribution.

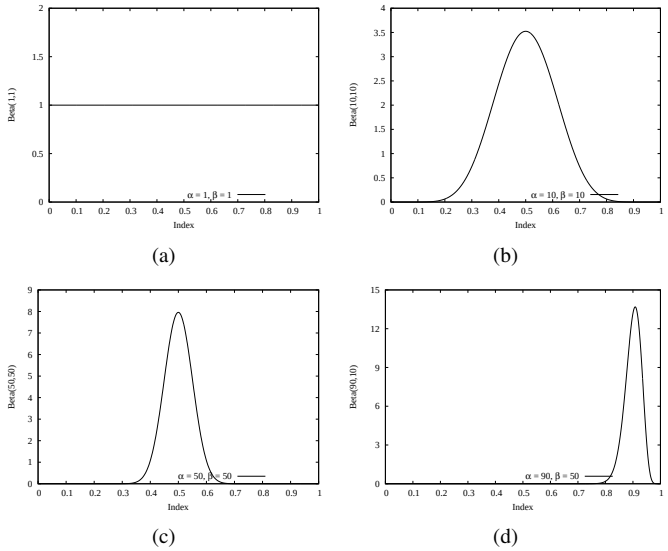


Fig. 2. (a) $Beta(1, 1)$, (b) $Beta(10, 10)$, (c) $Beta(50, 50)$, (d) $Beta(90, 10)$. Corresponding b, d, u representation see Fig. 1.

There are two important attributes for uncertainty. First, when $(\alpha+\beta)$ is higher, it implies that there is more evidence, which consequently lowers uncertainty u. Second, when the evidence for success or failure dominates, there will be less uncertainty when compared to the situation in which there is equal evidence for both success and failure. This is because, for any given $(\alpha + \beta)$, uncertainty u will be at its peak when $\alpha = \beta$. Therefore, we define uncertainty u as the normalized variance of $Beta(\alpha, \beta)$ as follows:

Definition 1: (Uncertainty Computation) Let uncertainty be the normalized variance of the Beta function:

$$u = \frac{12 \cdot \alpha \cdot \beta}{(\alpha + \beta)^2 \cdot (\alpha + \beta + 1)}$$

The numerator and denominator in Formula 1 guarantee the latter and the former attributes respectively.

The total certainty is $(1 - u)$ which can be divided into b and d according to their proportion of supporting evidence. Since the proportion of supporting evidence for the statement that the transmission between two nodes is reliable is $\frac{\alpha}{(\alpha+\beta)}$, b can be calculated as follows: $b = \frac{\alpha}{(\alpha+\beta)} \cdot (1-u)$. Therefore, $d = (1 - u) - b = \frac{\beta}{(\alpha+\beta)} \cdot (1 - u)$.

D. Second-hand Information Integration

Using first-hand information alone is not cost effective. Reputation exclusively based on direct contact increases the detection time when compared to an approach that also uses reports from others. The more information each node considers, the faster the trust evaluation achieves convergence.

Second-hand information is the information that a node gets from the first-hand information published by other nodes. It is a kind of trust transitivity. Node A first gathers other nodes' first-hand observations (in α, β) towards node C. Node

A converts the information (in α, β) into an opinion (in b, d, u) and discounts it by node A's opinion towards the node reporting the observation. We call this the recommendation calculation. After gathering all the recommendations, node A will synthesize them and integrate the second-hand information with the first-hand observation and make a final anticipation and decision.

Definition 2: (Recommendation Calculation) Let $R_C^B = \{b_C^B, d_C^B, u_C^B\}$ represent node B's opinion towards C, and $R_B^A = \{b_B^A, d_B^A, u_B^A\}$ represent node A's opinion towards B. Then node A will take node B's recommendation towards node C as $R_C^{A:B} = \{b_C^{A:B}, d_C^{A:B}, u_C^{A:B}\}$, where:

$$b_C^{A:B} = b_B^A \cdot b_C^B; \quad d_C^{A:B} = b_B^A \cdot d_C^B$$
$$u_C^{A:B} = b_B^A \cdot u_C^B + d_B^A + u_B^A$$

Definition 2 presents how node A computes the recommendation given by node B towards node C. Same formulas are used as the subjective logic [2] because they are both uncertainty centric and comply to common sense. Thus A's belief towards B's opinion is directly converted into A's belief, disbelief and uncertainty. Node A's disbelief in B's opinion becomes uncertainty towards C rather than becoming disbelief towards C. A's uncertainty in B also becomes part of the uncertainty in C. Notice that when node A's belief in B is high ($b_B^A \rightarrow 1$), the calculated recommendation will remain the same as B's opinion. The trust decay is low in this case as A trusts B.

Definition 3: (Recommendation Synthesization) Let $R_C^{A:B_i} = \{b_C^{A:B_i}, d_C^{A:B_i}, u_C^{A:B_i}\}$ represent node B_i's recommendation towards node C computed by node A, for $1 \leq i \leq n$. Then node A will synthesize these recommendations as $R_C^{A:\{B_1,...,B_n\}} = \{(b_C^{A:B_1} + ... + b_C^{A:B_n})/n, (d_C^{A:B_1} + ... + d_C^{A:B_n})/n, (u_C^{A:B_1} + ... + u_C^{A:B_n})/n\}$.

A simple method to calculate the average is used to synthesize the recommendations from different nodes towards one particular node. As is shown in the following example, this weighted average process makes the model resilient to false praise and accusation. When a misbehaving node's recommendation is highly different from other nodes, it will raise the trustor's uncertainty.

Definition 4: (Opinion Combination) Let γ be a node's character factor. Each node A will combine its first-hand and second-hand opinion towards B as:

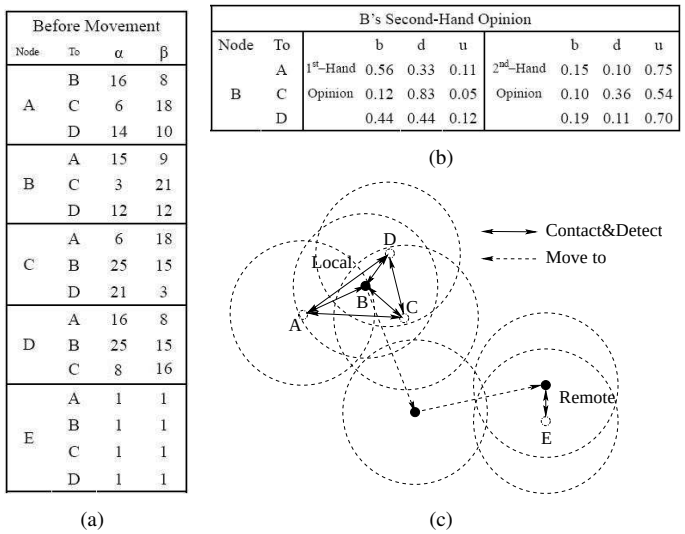
$$x_B^{A_f} = \phi_1 \cdot x_B^{A^{1st}} + \phi_2 \cdot x_B^{A^{2nd}}$$

where $x \in \{b, d\}$, $u_B^{A_f} = 1 - b_B^{A_f} - d_B^{A_f}$, and

$$\phi_1 = \frac{\gamma \cdot u_B^{A^{2nd}}}{(1-\gamma) \cdot u_B^{A^{1st}} + \gamma \cdot u_B^{A^{2nd}} - 0.5 \cdot u_B^{A^{1st}} \cdot u_B^{A^{2nd}}}$$

$$\phi_2 = \frac{(1-\gamma) \cdot u_B^{A^{1st}}}{(1-\gamma) \cdot u_B^{A^{1st}} + \gamma \cdot u_B^{A^{2nd}} - 0.5 \cdot u_B^{A^{1st}} \cdot u_B^{A^{2nd}}}$$

If γ is greater than 0.5, it means a node tends to trust it own experience. If γ is less than 0.5, it means a node tends to trust others' recommendations. In this equation $u_B^{A^{1st}}$ and $u_B^{A^{2nd}}$ are also two important factors. When the trustor is uncertain about one thing it tends to learn from others' opinions with less uncertainty. Otherwise its belief tends to be firm and others' opinions are less influential. ϕ_1 and ϕ_2 are composit factors which reflects the combined final weight.



Before Movement

Node	To	α	β
A	B	16	8
	C	6	18
	D	14	10
B	A	15	9
	C	3	21
	D	12	12
C	A	6	18
	B	25	15
	D	21	3
D	A	16	8
	B	25	15
	C	8	16
E	A	1	1
	B	1	1
	C	1	1
	D	1	1

(a)

B's Second-Hand Opinion

Node	To		b	d	u		b	d	u
B	A	1st–Hand	0.56	0.33	0.11	2nd–Hand	0.15	0.10	0.75
	C	Opinion	0.12	0.83	0.05	Opinion	0.10	0.36	0.54
	D		0.44	0.44	0.12		0.19	0.11	0.70

(b)

(c)

Fig. 3. (a) Results of first-hand observation, (b) Node B's first- and second-hand opinion, (c) Node B's movement.

E. Example

Fig. 3 illustrates the model. Four nodes A, B, C and D are close to each other. They make contact with each other and obtain low uncertainty local trust. We assume each pair of nodes contacts 22 times. Fig. 3 (a) presents the first-hand α, β of each node. Each node also broadcasts its first-hand α, β in its neighborhood. In this example, we assume A and D are trustworthy nodes. C is untrustworthy. It gives false praise to D and false accusation to A.

We then examine B's activity. B converts α, β of its first-hand observation and other nodes' recommendation to b, d and u. It then combines recommended opinions and summarizes its second-hand opinion. As shown in Fig. 3 (b), the first- and second-hand opinion are both in accordance with nodes' behavior. The uncertainty in second-hand opinion is high because of C's false recommendations which lead to confusion. High uncertainty is coherent with common sense. Nodes A, C and D also conduct the same calculation.

When these local nodes need cooperation from some remote nodes, as they do not have adequate trust information, they need to employ mobility to reduce uncertainty. In this example, as B is the node with highest b and least u, it is selected to travel. After moving to the one-hop area of E, B interacts with E for long enough to reduce its u towards E to a certain threshold, and moves back to A, C and D's one-hop area. Then B broadcasts its α, β towards E. Because B is the common trusted node among these nodes, each node gets a second-hand opinion towards E from B's recommendation with relatively low uncertainty.

IV. Mobility for Uncertainty Reduction

Node movement increases the chance for potential contactors to gather more trust information and evidence, thus enlarging the scope of reputation qualified candidate nodes for future tasks. We present a detailed discussion on the effect of mobility on uncertainty reduction in this section.

Assume that trust events happen at a uniform rate ρ between each pair of one hop neighbors. Each node's actual behavior is consistent and can be described as θ as in [6], which is the probability that a node will be honest in the trust events. A node's average moving speed is v. The moving cost per unit distance is c_m. The unit cost of the trust event (such as one message exchange) is c_e. We use the total cost and total convergence time to study the uncertainty reduction efficiency of each mobility model.

Here a theorem is established to continue the research. U_{max} is an uncertainty threshold that nodes are required to satisfy before we begin any trust based MANET application.

Theorem 1: (Pause Time) In each step, a pair of nodes should interact at least $\frac{3}{U_{max}}-1$ times to satisfy the uncertainty threshold requirement.

Proof: We require: $u \leq U_{max}$ and compute u as in Definition 1. We use $x = \alpha + \beta$ to represent total number of interactions. For a given x, when $\alpha = \beta = \frac{x}{2}$, u achieves maximality. So $x \geq \frac{3}{U_{max}} - 1$ guarantees that $u \leq U_{max}$. ■

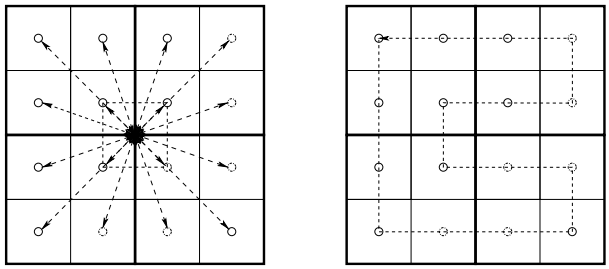
A. The Effect of Random Waypoint Model

First, we analyze the effect of mobility based on a realistic model: random waypoint model. Using this model, nodes will have a new neighborhood during each pause time. A node can contact and observe its new neighbors directly. The results of these direct contacts increase the α or β in both nodes' first-hand opinion, therefore reducing uncertainty. However, the randomness also restricts the use of second-hand information. In each pause time, the disbelief and uncertainty between the newly encountered nodes are uncontrollable. In most cases, the recommendations from the new neighbors are useless. Hence the trust information propagation mechanism in our reputation system is not fully utilized. Applications such as reputation based routing are also hard to deploy under this model.

B. The Effect of Controlled Mobility Models

We analyze and design controlled mobility models based on the features of the recommendation and integration process in the reputation system to fully utilize second-hand information propagation.

Assume a grid-based model of size $2^k \times 2^k$. All the nodes in a 1×1 grid form a cluster. Although the basic model can be easily converted to other models, the grid-based model is chosen for its simplicity. Set the wireless communication range as 1 unit distance. Each node in a cluster knows which grid it belongs to and the number of nodes in the same cluster. Use N to represent the number of grids in the network, $N = 2^k \times 2^k = 4^k$. Each grid has n nodes. We first analyze and compare two straightforward controlled movement models:



(a) (b)

Fig. 4. (a) Town hall model, (b) Traveling preacher model.

1) Town Hall Model: The first straightforward model is shown in Fig. 4 (a): all nodes in the network travel to one grid, pause for a sufficient time, build up trust, and reduce the uncertainty of other nodes to a required degree. After that, all nodes move back and will be able to perform tasks that demand remote nodes to cooperate and have trust requirements. We can approximate this model as all nodes start moving from the center of their grid, to the center of the network, pause for some time, and move back.

If this model is analyzed under the above settings, we have the total moving distance as $8^k \cdot n$ and the number of interactions as $C^2_{4^k \cdot n} \cdot (\frac{3}{U_{max}} - 1)$. Therefore the total cost is $8^k \cdot n \cdot c_m + C^2_{4^k \cdot n} \cdot (\frac{3}{U_{max}} - 1) \cdot c_e$; The moving time (round trip) is $\frac{2^k}{v}$ and the pause time is $(\frac{3}{U_{max}} - 1)/\rho$. The convergence time is $(\frac{3}{U_{max}} - 1)/\rho + \frac{2^k}{v}$. The town hall model will lead to relatively short convergence time with extremely high cost.

2) Traveling Preacher Model: Another straightforward model is to select one common trusted node to travel around all the grids through a Hamiltonian path, as shown in Fig. 4(b). That node's movement can be divided into two rounds. In the first round, it pauses in each grid for a sufficient time to collect trust information. In the second round, it travels to each grid again to disseminate all the gathered trust information about other grids using the recommendation mechanism.

An important issue in this model is how to select the moving node. One possible method is to let the system assign one node to be the moving node, and all other nodes should assign $b = 1$ to that moving node. But, this violates the self-organized rule of MANETs. Another option is to let the nodes elect one node that satisfies some condition to travel around. We will discuss the detailed election scheme later.

Using this model, the total moving distance is $2 \cdot 4^k$, the number of interactions is $4^k \cdot n \cdot \frac{3}{U_{max}}$. So, the total cost is $2 \cdot 4^k \cdot c_m + 4^k \cdot n \cdot \frac{3}{U_{max}} \cdot c_e$; The moving time is $\frac{2 \cdot 4^k}{v}$ and the pause time is $(4^k \cdot \frac{3}{U_{max}})/\rho$. Therefore the convergence time is $\frac{2 \cdot 4^k}{v} + (4^k \cdot \frac{3}{U_{max}})/\rho$. Traveling preacher model shows a relatively long convergence time but extremely low cost.

C. Mobility Assisted Uncertainty Reduction Scheme

When the requirement is a short convergence time to quickly start a trust-based application, or a controllable cost, the above two mobility models will offer extreme options. However,

these two methods are not flexible enough and we lack a way to find a tradeoff between convergence time and cost to satisfy different application objectives. Here we present a two-level controlled mobility model which is called MAURS. In MAURS, we divide the whole network into several regions, allowing each region to contain a specified number of grids, and choose mobility models for intra- and inter-region movement. MAURS combines the advantages of the above two models and offers more options for MANET implementation. The design of the MAURS consists of the following three parts:

1) Moving Node Election: After the cluster has been set up, all the nodes in the cluster will contact each other locally, build up trust, and compute reputation according to the previously discussed reputation system. After a sufficient pause time, each node will vote for the node with the largest belief and smallest uncertainty to move. The voting process can be described as Algorithm 1. Here B_{min} is the belief threshold. λ is the required proportion of votes to win an election. U_{max}, B_{min} and λ should be regulated in the clusters' voting policy and represent the reputation requirements for a moving node. Each node sets a pause timer and will cast only one vote after timeout.

Algorithm 1 VoteForMove

```
while the timer lasts do
    if an event occurs then
        Get first-hand observation and change α, β accordingly;
    end if;
    if a recommendation comes then
        Update second-hand opinion accordingly;
    end if;
end while;
Compute combined opinion b, d, u for each node;
if the largest b in all the opinions satisfy b ≥ B_min then
    Vote the node with the largest b;
    Wait for the confirmation from elected moving node;
else
    Continue trust information collection;
end if;
```

As described in Algorithm 2, a node should wait until it gathers enough votes to move. It will go through a defined trajectory to collect the trust information for its home cluster.

Algorithm 2 VoteGathering

```
Vote counter+1 when a vote comes;
if vote counter ≥ λ proportion of the nodes in the cluster then
    Node broadcasts an elected confirmation and starts to move;
end if;
```

Nodes have already been organized into clusters based on which grid they belong to. The network is then divided into a number of regions. Each region selects one grid to be its "capital". All of the elected moving nodes move to the capital of the region.

The moving nodes will repeat the local contact process after they arrive in the capital. The pause time period in the capital allows them to build trust between each other and the local nodes of the capital. One node which is commonly trusted by all moving nodes will be elected to be the "keeper" of that region through a process similar to Algorithm 1 and 2. The keeper will select several nodes it trusts as "ambassadors" which will travel between regions to collect information and feed it back to the keeper.

2) Region Partition: The election process creates different roles to handle different trust information collection and dissemination tasks for intra-grid, intra-region and inter-region. As we will use different methods to handle different classes of tasks, how to partition the region becomes an important design issues. The analysis of the town hall and traveling preacher models show that the cost in the town hall model is positively proportional to the square of the number of moving nodes, while the total pause time of the traveling preacher model is decided by the number of stops. To offer a more flexible uncertainty reduction oriented mobility model, we can choose an optimal number of regions based on node density, network scale, and application related cost and convergence time objectives. For a $2^k \times 2^k$ network, $2^0 \times 2^0, 2^1 \times 2^1$ till $2^k \times 2^k$ are possible region sizes. We can compute the convergence time and cost for each of these possible region sizes and select the optimal one as the scheme for region partition.

3) Moving Pattern control: As we divide the network into regions consisting of grids, an optimal moving pattern for the inter- and intra-region levels must be selected.

For the intra-region level, we select an extension of the town hall method. Each grid elects a commonly trusted moving representative, and these nodes move to the capital to exchange intra-region trust information.

For the inter-region level, a method will be chosen according to the number of regions and the distance between capitals. Possible moving patterns for inter-region level are town hall, traveling preacher and another straightforward model which we call *exchange ambassadors*. Using the town hall model will largely increase the uncertainty decay in recommendations from other regions. Considering a limited number of regions, an extension of traveling preacher model can be applied and the time burden will be acceptable. In this extension, each region sends an ambassador to travel around the capitals and collect information only for its home region. Exchange ambassadors means each pair of regions exchange ambassadors which collect trust information for their home regions. It is a high cost and low convergence time method and is especially suitable for a small number of regions. The main problem with this method is the ambassador selection. The keeper may not be able to find as many trustable ambassadors as it needs from the capital.

D. Analysis for the MAURS

The MAURS offers many ways to adjust the convergence time and total cost related to a specific certainty goal. We will analyze the general convergence time and cost under a certain requirement U_{max}, and the general trust decay.

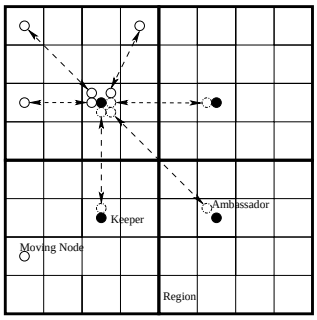


Fig. 5. A two-level mobility assisted uncertainty reduction scheme.

Theorem 2: (Trust Decay) When the moving node goes back to its home cluster, the upper bound of uncertainty on the λ portion of nodes that voted for the moving node is:

$$u \leq 1 - B_{min} + B_{min} \cdot \frac{3}{\rho \cdot T_p + 1}$$

Proof: Based on Algorithm 1 and 2, the moving node is approved by at least λ percentage nodes in the home cluster. For these nodes, the opinion b, d, u towards the moving node should satisfy $b \geq B_{min}$ and $u \leq U_{max}$. The moving node broadcasts its first-hand observation α, β for the place of interest. T_p represents the moving node's pause time in the place of interest, and we have $\alpha + \beta = \rho \cdot T_p$.

Each node in the home cluster has no previous knowledge about the remote interest node, so for the ordinary nodes in the home cluster $u^{1^{st}} = 1$. From Definition 1, when $\alpha = \beta = 0.5 \cdot \rho \cdot T_p$, the uncertainty in the moving node's broadcast opinion will achieve a maximum. Using Definition 2 to compute the recommendation opinion from a moving node, $u^{2^{nd}} = b \cdot u_m^{1^{st}} + d + u$. As $b \geq B_{min}$ and $d + u = 1 - b$, for those nodes who vote for the moving nodes $u^{2^{nd}} = 1 - b \cdot (1 - u_m^{1^{st}})$. Because $u^{1^{max}} = 1$ and using Definition 4, we get: $u \leq 1 - B_{min} + B_{min} \cdot \frac{3}{\rho \cdot T_p + 1}$ for all the nodes who vote for the moving node. ■

From Theorem 2 it can be seen that the upper bound for the uncertainty of the remote interest node after the moving node comes back and broadcasts its observation is decided by two factors. The first one is a base uncertainty $1 - B_{min}$, which is decided by B_{min}, the threshold belief for moving. This B_{min} is decided by the policy of the MANET. This requirement can be satisfied if nodes' actual behavior factor θ complies to normal distribution and the number of nodes n in a cluster is large enough. For the second part of uncertainty $B_{min} \cdot \frac{3}{\rho \cdot T_p + 1}$, the longer the pause time of the moving node in a remote interest place, the smaller the uncertainty will be.

We now choose town hall and exchange ambassadors schemes for intra- and inter-region movement and select the number of regions as 4^i. Theorem 3 and 4 show the factors that we can adjust to achieve certain convergence time and cost objectives.

Theorem 3: (Convergence Time) Given an uncertainty requirement U_{max}, the convergence time can be described as:

$$T = \frac{2^{k+2} \cdot (1 - 2^{-i})}{v} + \frac{9}{U_{max} \cdot p}$$

Proof: The total convergence time will include 3 pause periods and 2 moving periods. The 3 pause periods include the local election period, moving nodes' pause time in the capital, and ambassadors' pause time in foreign capitals. The ambassadors will go back to the home capital and broadcast once. The moving nodes will do the same thing in their local grid. According to Theorem 1, all the 3 pause periods should satisfy the U_{max} requirement. The total pause time should be: $T_p = 3 \cdot \frac{3}{U_{max} \cdot p} = \frac{9}{U_{max} \cdot p}$.

The moving time includes the time for moving nodes to travel to the capital and back, and the time for ambassadors to travel to the foreign capitals and move back. We will compute the travel time for the farthermost grid/foreign capital. The travel time is $\frac{2 \cdot (2^{k-i} + 2 \cdot 2^k - 2 \cdot 2^{k-i})}{v} = \frac{2^{k+2} - 2^{k-i+2}}{v}$. ■

Theorem 4: (Total Cost) Given uncertainty requirement U_{th}, the total can be described as:

$$C = 4^i \times ((8^{k-i} + 2^{k-4}) \cdot c_m + (\frac{n \cdot (n-1) + 4^{k-i} \cdot (4^{k-i} - 1)}{2} + 4^k) \cdot (\frac{3}{U_{max}} - 1) \cdot c_e)$$

Proof: For each region, the cost of trust events happening during the moving node selection period of each grid should be: $\frac{n \cdot (n-1)}{2} \cdot (\frac{3}{U_{max}} - 1) \cdot c_e$.

Each region contains $2^{k-i} \times 2^{k-i}$ grids. 4^{k-i} elected moving nodes will move to the capital. Similarly, we can get the cost of interactions between the moving nodes. The cost for intra-region movement is: $8^{k-i} \cdot c_m$. So the total cost for the intra-region should be: $C_{intra} = 4^i \times (8^{k-i} \cdot c_m + (\frac{n \cdot (n-1) + 4^{k-i} \cdot (4^{k-i} - 1)}{2}) \cdot (\frac{3}{U_{max}} - 1) \cdot c_e)$.

Each region will send out $4^i - 1$ ambassadors and one keeper. The cost of inter-region movement should be: $C_{inter} = 2^{k+2i-4} \cdot c_m + 4^{k+i} \cdot (\frac{3}{U_{max}} - 1) \cdot c_e$. ■

Theorem 3 and 4 illustrate that the way in which the network is partitioned decides the convergence time and cost. By adjusting i in the above equations, a trade-off between the convergence time and cost can be found.

The trust opinion for nodes in the same region (except the home grid and the capital) will go through 3 hops. For nodes in different regions, the opinion will go through 4 hops. Whenever a trust opinion goes through one more hop, the uncertainty will at least increase $1 - B_{min}$ where B_{min} can be different for each layer. If there are more than 2 layers in the hierarchical moving model, the uncertainty will be high.

V. Implementation Issues

In this section, we investigate the implementation of controlled mobility, study the resilience of the proposed reputation system as well as challenges which makes its implementation more complex.

(Controlled Mobility) Although the moving patterns of most nodes in the MANET are considered to be naturally random and independent of each other, controlled the moving trajectory and rendezvous points of a small portion of nodes to achieve better performance are considered to be possible

in many recent research papers such as [17].In MAURS, the moving trajectory and rendezvous points of the elected nodes are planned before moving. This does not contradict with the motive and properties of MANETs. Furthermore, the voting process could be replaced by random node selection.

(General Attacks and Protection) Attacks, such as bad mouthing and faked identity, are considered as general problems in current trust systems. As mobility are exploited to help trust convergence, the characteristics and influence of these attacks also changes.

Bad mouthing attack means malicious parties provide dishonest recommendations of other nodes. In our work, the defense against this attack is two folds: First, the published second-hand observation is discounted by the trustor's opinion towards the recommender. Second, in the voting process, we establish criteria to guarantee that only common trusted nodes will move and collect remote nodes' reputation information.

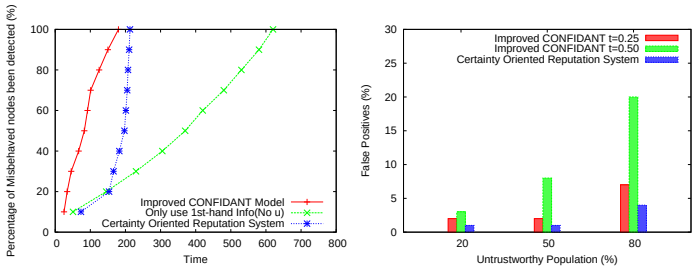
If a malicious node can create several faked IDs, the trust management system suffers from the sybil attack [18]. We can partly solve this problem through imposing a strong uncertainty requirement. As the attacker uses several different identities to apportion its bad reputation and given the same total contact interval, the uncertainty must be higher than other nodes. Mobility will also make a Sybil attack more severe, as mobility may also help the attacker to renew its identity.

(Behavior Inconsistency) In implementation, a node's behavior may not be consistent. On one hand, an incompetent node may become competent due to environmental changes. On the other hand, malicious nodes may alternate their behavior between good and bad, hoping that they can remain undetected. One widely used method in existing trust systems to deal with this problem is to use an aging factor. However, designing the aging factor is more complicated when we consider mobility. As the moving node needs time to gather a remote interest place's trust information, its local belief will get a discount and the uncertainty in its recommendation will go up. Using number of events driven reputation discount will be better for this system.

VI. Simulation Evaluation

In simulation, we aim to investigate the robustness of our uncertainty oriented reputation system and the effects of different mobility models on the uncertainty reduction. All approaches are simulated on a custom simulator, which generates random initial deployment. We set up the simulation in $2^k \times 2^k$ ($k = 0, 3$, and 10 in different experiments) square area in which nodes are evenly deployed. In each experiment, the simulation lasts 500 rounds and the results are collected and averaged.

For the first experiment, we deploy 100 nodes in a 1×1 gird. The performance metrics are the detection efficiency and the number of false positives. There are three reputation systems to compare. In these systems, detected means a node is classified as a misbehaving node ($d \geq 0.4$) by all normal nodes. From Fig. 6 we can see that improved CONFIDANT [6] is more efficient than using only first-hand information when we set



(a) (b)

Fig. 6. (a) Detection efficiency, (b) False positives.

the second-hand weight $w = 0.1$, and the update threshold $t = 0.25$. Our reputation system (character factor $\gamma = 0.6$) is less efficient then the other two methods in the initialization time period, as the uncertainty is high and the disbelief can not reach the threshold. But when uncertainty is reduced and with the efficient use of second-hand information, the detection ratio goes up quickly. If we also take the number of false positives into account, as [6] produces more false positives when $t = 0.25$, the certainty oriented reputation system is certainly a good choice.

Several factors strongly influence the uncertainty reduction efficiency. We use different mobility models and adjust the main parameters in the simulation. These parameters include: network size ($2^k \times 2^k$ grids, each grid has n nodes); threshold for belief (default: $b_{min} = 0.6$); threshold for uncertainty (default: $u_{max} = 0.3$); required proportion of votes to win an election (default: $\lambda = 0.7$); interaction ratio (default: $\rho = 10$); nodes' moving speed (default: $v = 0.5$); unit cost for moving (default: $c_m = 1.0$); unit cost for one interaction (default: $c_e = 1.0$). The observation value of this simulation are the convergence time and total cost.

For Fig. 7 (a) to (d), we set up $2^3 \times 2^3$ grids, each has $n = 16$ nodes. We compare four different mobility models: the town hall model, traveling preacher model and MAURS with region size 4 and 16. Random waypoint model is also considered and compared under different moving speed and interaction ratio. We may draw these conclusions from Fig. 7 (a) to (d): 1) Town hall and traveling preacher models are two extreme cases. Town hall model has the smallest convergence time and largest total cost while traveling preacher model causes huge convergence time and has the lowest total cost; 2) Under Random waypoint model, the convergence time is also acceptable. But MAURS leads to shorter convergence time in most of the simulation cases; 3) MAURS offers a good trade-off between total cost and trust convergence time. In all the cases, the curve of the MAURS is close to the best extreme case; 4) Different region size leads to different performance in MAURS. In this simulation experiment, MAURS with region size 4 outperforms MAURS with region size 16 in both convergence time and total cost. We use a network size $2^{10} \times 2^{10}$ grids in Fig. 7 (f) to (g) and vary the number of regions from 4^0 to 4^{10}. $i = 0$ represents the extension of the town hall model. The environmental variable v and the

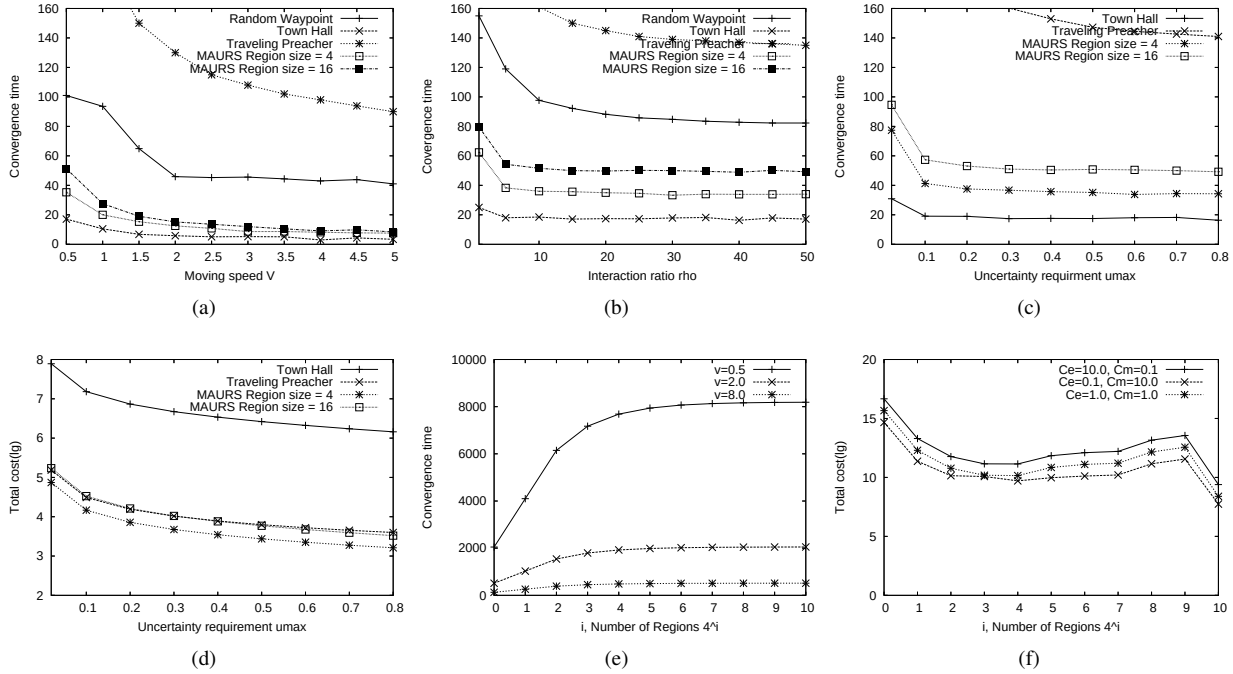


Fig. 7. Convergence time with different (a) moving speed v, (b) interaction ratio ρ, and (c) uncertainty requirement U_{max}; Total cost with different (d) uncertainty requirement U_{max}; (e) Convergence time with different number of regions 4^i, (f) Total cost with different number of regions 4^i.

weight between c_e/c_m have strong influence on the slope of each curve. Therefore, the application objectives (cost or time sensitive) together with v and c_e/c_m decide the optimal number of regions.

VII. Conclusion

Uncertainty is one core dimension of trust, which reflects a node's confidence in the sufficiency of past experiences. It deeply impacts nodes' anticipation and decision. In this paper, we present a certainty oriented reputation system that emphasizes the relationship among uncertainty, observation and recommendation. This system uses mobility as an asset to reduce uncertainty in far-flung nodes, and reduce the overall uncertainty in the network. We give both theoretical proof and simulation results to illustrate that our approach strikes an acceptable balance between the cost and convergence time.

In the future, we will further study the small-world model under our reputation system, conduct simulation and analytical research to find ways to organize nodes based on node degree and trust value, so that nodes can be grouped with nodes that they trust to form high-trust clusters.

References

[1] S. Kamvar, M. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proc of WWW*, pages 640–651, 2003.

[2] A. Josang. An algebra for assessing trust in certification chains. In *Proc of the Network and Distributed Systems Security (NDSS'99) Symposium*, 1999.

[3] Y. Sun, Z. Han, W. Yu, and K. Liu. A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. In *Proc of the IEEE INFOCOM*, 2006.

[4] M. Carbone, M. Nielsen, and V. Sassone. A formal model for trust in dynamic networks. In *BRICS Report RS-03-4*, 2003.

[5] S. Ganeriwal and M. Srivastava. Reputation-based framework for high integrity sensor networks. In *Proc of the ACM SASN*, pages 66–77, 2004.

[6] S. Buchegger and J. Boudec. Performance analysis of the confidant protocol. In *Proc of MobiHoc*, pages 226–236, 2002.

[7] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Communications and Multimedia Security*, pages 107–121, 2002.

[8] S. Bansal and M. Baker. Observation-based cooperation enforcement in ad hoc networks. *CoRR*, cs.NI/0307012, 2003.

[9] S. Buchegger and J. Boudec. A robust reputation system for p2p and mobile ad-hoc networks. In *Proc of the Second Workshop on the Economics of Peer-to-Peer Systems*, 2004.

[10] A. Joang, S. Marsh, and S. Pope. Exploring different types of trust propagation. In *Proc of the 4th International Conference on Trust Management(iTrust)*, 2006.

[11] A. Josang and S. Pope. Normalising the consensus operator for belief fusion. In *Proc of the International Conference on Information Processing and Management of Uncertainty (IPMU2006)*, July 2006.

[12] T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502, 2002.

[13] J. Wu, S. Yang, and F. Dai. Logarithmic store-carry-forward routing in mobile ad hoc networks. accepted to appear in *IEEE Transactions on Parallel and Distributed Systems*, 2007.

[14] S. Capkun, M. Cagalj, and M. Srivastava. Securing localization with hidden and mobile base stations. In *Proc of the IEEE INFOCOM*, 2006.

[15] S. Capkun, J. Hubaux, and L. Buttyán. Mobility helps security in ad hoc networks. In *Proc of the ACM MobiHOC*, June 2003.

[16] W. Zhang, H. Song, S. Zhu, and G. Cao. Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks. In *Proc of MobiHoc*, pages 378–389, 2005.

[17] W. Zhao, M. Ammar, and E. Zegura. A message ferrying approach for data delivery in sparse mobile ad hoc networks. In *Proc of the ACM MobiHoc*, pages 187–198, 2004.

[18] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proc of IPSN*, pages 259–268, 2004.